BUFFER MANAGEMENT FOR
MOBILE INTERNET PROTOCOL

Inventors: Mohamed Khalil
                  Dallas, TX
                  citizen of U.S.

                  Emad A. Qaddoura
                  Plano, TX
                  citizen of U.S.

                  Haseeb Akhtar
                  Garland, TX
                  citizen of U.S.

Assignee: Nortel Networks, Limited
                  380 St. Antoine Street West, 8th Floor
                  Montreal, Quebec H2Y 3Y4
                  Canada

BUFFER MANAGEMENT FOR MOBILE INTERNET PROTOCOL

Cross Reference

This application claims the benefit of U.S. Ser. No. 60/160,031 filed October 18, 1999.

Technical Field

5   This invention relates generally to management techniques for a wireless communications network and, more particularly, to a system and method for facilitating the seamless transfer of data to a mobile node as the mobile node roams in a mobile internet protocol network.

Background

There are many emerging trends in the communications world, including the increase in mobile network technology and the rise in packet data networks. There are many types of mobile network technologies, including global systems mobile ("GSM"), code

15   division multiple access ("CDMA"), time division multiple access ("TDMA"), and advanced mobile phone service ("AMPS"). Likewise, there are many types of packet data technologies, such as asynchronous transfer mechanism ("ATM") and internet protocol ("IP"). Packet data technologies send packets of data, or datagrams, in which sections of a message are transmitted in scattered order and then re-ordered at a receiving node.

20   Mobile IP is an emerging "layer 3" type protocol that allows a mobile node to establish a wireless connection to an IP network. Mobile IP essentially has three major subsystems. A first subsystem is a discovery mechanism that provides mobile nodes with new attachment points (new IP addresses) as they move within the IP network. A second subsystem allows the mobile node to register with its "home network" when it learns its new

IP address. A home network is a network, possibly virtual, that has a network prefix matching that of the mobile node's "home address." A home address is an IP address that is assigned for an extended period of time to the mobile node. It remains unchanged regardless of where the mobile node is attached. Standard IP routing mechanisms will deliver packets

5 destined to a mobile node's home address to the mobile node's home network.

A third subsystem allows data to be directed to the mobile node when it is away from its home network by using the registered IP address. For the sake of reference, mobile IP is discussed in greater detail in the book Charles E. Perkins, MOBILE IP: DESIGN PRINCIPLES AND PRACTICES (Computer & Engineering Publishing Group ISBN: 0-201-63469-4, 1998).

10 In each of these systems, packets of information are often lost when a mobile node during handoff. What is needed is a system and method to reduce the number of lost packets when a mobile node hands-off from one agent to another.

Summary

15 The present invention provides a buffer management method for a mobile node in a telecommunication network. In one embodiment, the method supports a handoff of the mobile node from a first agent of a first network to a second agent of a second network. The method begins upon initiation of the handoff. A first message is sent to the first agent requesting the first agent to buffer any packets being sent to the mobile node. While the

20 buffering is being performed, the handoff may be completed to the second agent. Once the handoff is complete, a second message can be sent to the first agent requesting the first agent to forward the buffered packets to the second agent.

A technical advance is achieved because the packets of information are buffered as a mobile node changes its network point of attachment, thereby reducing the possibility of lost

25 data packets.

Another technical advance is achieved by reducing an overall amount of buffering being performed by either agent.

Brief Description of the Drawings

30 Fig. 1 is a simplified description of several typical wireless networks and agents in which one or more embodiments of the present invention may be employed.

Figs. 2-4 are flow charts for messages used to facilitate a handoff of a mobile node from one agent to another.

Figs. 5-9 are messages, such as can be used in the flow charts of Figs. 2-4.

5

Detailed Description

The present disclosure relates to buffer management, such as can be used for mobile internet protocol. It is understood, however, that the following disclosure provides many different embodiments, or examples, for implementing different features of the invention. Specific examples of components, messages, sequences and arrangements are described

10 below to simplify the present disclosure. These are, of course, merely examples and are not intended to limit the invention from that described in the claims.

The following discussion is divided into seven different sections. The first section describes exemplary networks that may benefit from the present invention. The second section describes basic handoff scenarios for a mobile node in the exemplary networks. The

15 third section describes messages and extensions for use in the handoff scenarios. The fourth and fifth sections describe unique considerations for the mobile node and a foreign agent, respectively. The sixth section describes buffer management for performing the handoff scenarios. Finally, the seventh section provides a conclusion.

20 Exemplary Networks

Referring now to Fig. 1 of the drawings, the reference numerals 10, 12, and 14 refer, in general, to simplified conventional mobile IP packet networks. The networks 10, 12, 14 allow a mobile node (MN) 16 to wirelessly communicate with a correspondence node 18, which may be wired or wirelessly connected to the networks. The MN 16 includes hardware

25 components like a conventional wireless device, including a processor, memory, and an interface, for wirelessly connecting to another node. The network 14 is, in the present example, the home network for the MN 16, and maintains current location information for the MN 16 and delivers packets to the MN 16 when it is in away. The MN 16 includes the necessary components to establish a wireless connection to the networks 14 through a home

30 agent (HA) 14a. The HA 14a is a node of the network 14, and includes a conventional amount of processing, memory, and switching capacity.

When away from its home network, the HA 14 provides a "care-of address" for the MN 16. A care-of address is a termination point of a tunnel for packets forwarded to the MN 16 while it is away from home. There are two different types of care-of address: a foreign agent care-of-address is an address of a foreign agent with which the MN 16 is

5 registered, and a collocated care-of address is an externally obtained local address associated with one of its own network interfaces. When the MN 16 is away from home, it registers its care-of address with its HA 14. The MN 16 uses its home address as the source address of all IP packets that it sends, except where otherwise required.

The MN 16 may roam by establishing wireless (or wireline) connections with various

10 foreign agents (FAs). A foreign agent is a router node in a "visited" foreign network which cooperates with the home agent to complete the delivery of packets to the mobile node while it is away from home. Each FA includes a conventional amount of processing, memory, and switching capacity. A visited foreign network is a network other than a mobile node's home network, to which the mobile node is currently connected. Each foreign agent maintains a

15 visitor list of all the visiting mobile nodes.

For the sake of example, FAs 10a, 12a of networks 10, 12, respectively, are illustrated. The mobile node may roam to a location "A" and establish a wireless connection with foreign agent 10a in network 10, and then may roam to a location "B" and establish a wireless connection with foreign agent 12a in network 12.

20 When the MN 16 is roaming (for instance, at position A), packets sent to the mobile node's home address are intercepted by the home agent 14a, tunneled to the care-of address, received at the tunnel endpoint (FA 10a), and finally delivered to the mobile node. In the reverse direction, packets sent by the MN 16 are generally delivered to their destination using standard IP routing mechanisms, not necessarily passing through the home agent 14a.

25 Mobile IP has a process called "IP Security." IP security is a tunneling security context between a pair of nodes. For example, IP Security may use a Security Parameters Index for identifying a security context between a pair of nodes among the contexts available in the mobility security association.

Security and Smooth handoff with minimal data loss and delay are

30 desirable goals of any mobile network. Route Optimization techniques attempt to solve some of the issues related to smooth handoff, but difficulties still arise. Additionally, it may be necessary for the MN to authenticate the new FA before allowing it (the new FA) to

receive data from the previous FA. In such cases, the new FA is authenticated by the MN's Home Agent (HA) during the handoff.

For example, consider a communicating node (CN) 18 connected to the network 14. The CN 18 may be a computer server that is sending packets to the MN 16. Traditionally, when the MN 16 moves from point A to point B, FA 10a immediately begins to forward packets to FA 12a. This is a problem because handoff to the FA 12a may not be completed. This results in a breach of security because the FA 12a has not been authenticated. This also may result in a loss of one or more packets. To recover from the loss of one or more packets, the CN 18 must resend these packets, thereby degrading the general performance of the overall network.

Instead, the present invention decreases the window of data loss and delay during handoff. In particular, a new buffer management method minimizes the potential loss of data while the MN changes its network point of attachment. In addition, the buffer management method provides a way for the MN to verify the new FA during the handoff, if and when that is needed.

Basic Scenarios

In mobile IP, there are three basic types of handoff. The first type is called Mobile Assisted Handoff (MAH). In MAH, the Mobile Node (MN) discovers that it needs to move to a new FA and initiates the handoff. The second type is called System Assisted Handoff (SAH). In SAH, the new FA initiates the handoff after the MN sends a *Registration Request*. The third type of handoff is called *Previous FA Notification Extension Handoff* (PFANEH). In PFANEH, the MN starts the handoff process after entering the new FA. It is assumed that there is a security association between new FA and previous FA while performing PFANEH.

1. Mobile Assisted Handoff

Fig. 2 shows the message flow between the MN and the FA during a Mobile Assisted Handoff. Referring also to Fig. 1 for example, the MN 16 is roaming from a position A to a position B, and is being handed off from FA 10a ("Previous FA") to FA 12a ("New FA"). The following steps are performed in Fig. 2. These steps utilize certain messages which are described in greater detail below, with respect to Figs. 5-9.

(a)   A *Buffer Control Request* message is sent to the previous FA as soon as the MN discovers that it needs to move to the new FA. The previous FA starts to buffer data that are destined for the MN.

(b)   In some cases, the previous FA returns a *Buffer Control Response* message to the MN.

(c)   The MN moves to the new FA and sends a *Registration Request* message.

(d)   The new FA registers the MN and returns a successful *Registration Reply* message.

(e)   The MN sends a *Buffer Control Request* message to the previous FA requesting it to forward the buffered data.

(f)   In some cases, the previous FA returns a *Buffer Control Response* message to the MN.

During MAH, if the MN loses its direct communication (over the air) with the previous FA and fails to receive an expected *Buffer Control Response* message, the MN then should, in the present embodiment, change to either SAH or PFANEH mode (as described below) upon entering the new FA.

2. System Assisted Handoff

Fig. 3 shows the message flow between the MN and the FA during a System Assisted Handoff. Referring also to Fig. 1 for example, the MN 16 is roaming from a position A to a position B, and is being handed off from FA 10a ("Previous FA") to FA 12a ("New FA"). The following steps are performed in Fig. 3. These steps utilize certain messages which are described in greater detail below, with respect to Figs. 5-9.

(a)   The MN moves to the new FA and sends a *Registration Request* message with a *Buffer Control Request* extension.

(b)   The new FA sends a *Binding Update* message with a *Buffer Control Request* message to the MN. At this point, the new FA should start to buffer data that are destined for the MN.

(c)   In some cases, the previous FA sends a *Binding Acknowledgment* message with a *Buffer Control Response* extension to the new FA.

(d)   In some cases, the new FA forwards the *Binding Acknowledgment* message with the *Buffer Control Response* extension to the MN.

(e)   The new FA registers the MN and returns a successful *Registration Reply* message.

(f)   The MN sends a *Buffer Control Request* message to the previous FA requesting it to forward the buffered data.

(f)   In some cases, the previous FA returns a *Buffer Control Response* message to the MN.

During SAH, if a MN receives a successful *Registration Reply* message before an expected *Binding Acknowledgment* message from the previous FA, the MN should, in the present embodiment, wait for the *Binding Acknowledgment* message prior to executing step (f).

3. Previous FA Notification Extension Handoff

Fig. 4 shows the message flow between the MN and the FA during a handoff that uses Previous Foreign Agent Notification extension. Referring also to Fig. 1 for example, the MN 16 is roaming from a position A to a position B, and is being handed off from FA 10a ("Previous FA") to FA 12a ("New FA"). The following steps are performed in Fig. 4. These steps utilize certain messages which are described in greater detail below, with respect to Figs. 5-9.

(a)   The MN sends a *Registration Request* message to the FA (e.g., the previous FA) at the initial registration, with a *Buffer Control Request* extension. The FA allocates a buffer for the MN.

(b)   The FA (e.g., the previous FA) sends a *Registration Reply* message, which may include a *Buffer Control Response* extension, to the MN.

(c)   The MN moves to a new location and sends a *Registration Request* message to the new FA with a *Previous FA Notification* extension. It also adds two *Buffer Control Request* extensions: one for the new FA (with B = 1) to start buffering for the MN, and the other for the previous FA (with F = 1) so that it can forward the data to the MN. Both of these extensions may include other relevant information (*IP Filter* Extension, for example) pertaining to buffer management.

(d)   The previous FA creates a buffer for the MN and continues to buffer its data. This buffer is created according to the specification provided in the *Buffer Control Request* extension that was sent with the B bit set (B = 1). The new FA also sends a *Binding Update* to the previous FA with the *Previous FA Notification* extension as well as the *Buffer Control Request* extension that was sent with the F bit set (F = 1). The previous FA starts to forward data to the MN as soon as it receives the *Binding Update* message (according to the specifications provided in the *Buffer Control Request* extension).

(g)   The new FA registers the MN and returns a successful *Registration Reply* message, and may include a *Buffer Control Response* extension.

Messages and Extensions

In this section, a set of messages and extensions that are used in buffer allocation and management will be further described.

1. *Buffer Control Request Message*

This message is sent from the MN to the FA to allocate and manage data buffers for the MN. This message may be an individual message or may be added as an extension to *Registration Request* and *Binding Update* messages. This may be sent by the mobile node during registration (as an extension to the *Registration Request*) or it may be sent by the MN prior to (or as soon as) the discovery of handoff. This message is always sent to the FA. This message should, in the present embodiment, be implemented by both the FA and the MN for all of the scenarios (MAH, SAH and PFANEH) mentioned above.

The structure of this message is shown in Fig. 5. The flags are discussed below:

Type. This is for various type indications.

A. This flag indicates if the FA should allocate a buffer for the MN.

A = 0, allocate a buffer of default size (as decided by the FA).

A = 1, allocate a buffer of size defined in the *Buffer Size* extension.

B. This flag indicates if the FA should start buffering data that is destined for the MN. This should not, in the present embodiment, be set simultaneously with the F bit.

B = 0, do not buffer data.

B = 1, start to buffer data.

D. This flag indicates if the FA should stop buffering, deliver all the packets buffered so far, and then finally delete the buffer previously allocated for the MN.

D = 0, do not stop buffering or delete the MN's buffer.

D = 1, stop, deliver all packets buffered so far to the MN and then delete the

5 MN's buffer.

F. This flag indicates if the FA should forward data stored in the buffer to the MN. This should not, in the present embodiment, be set simultaneously with either B or K flag.

F = 0, do not forward the data.

F = 1, forward the data.

10 I. This flag indicates if the *Buffer Control Request* message has the Identification field.

I = 0, Identification field is not included.

I = 1, Identification field is included.

K. This flag indicates if the FA should send an acknowledgment(*Buffer Control*

15 *Response*) message to the MN.

K = 0, FA should not send any acknowledgment message.

K = 1, FA should send an acknowledgment message. Appropriate extensions should, in the present embodiment, be added if the FA can not allocate the buffer resources requested by the MN.

20 L. This flag indicates the type of the buffer.

L = 0, a fixed length buffer.

L = 1, a variable length buffer.

MN IP Address. The MN's home IP address.

Identification. An optional 64-bit number, constructed by the MN. It is used for

25 identifying the response to *Buffer Control Request* message. It is also used as protection a from replay attacks. It's included in the message if the I flag is set (I = 1).

2. *Buffer Control Response Message*

This message is sent from the FA to the MN in response to a *Buffer Control Request*

30 message. This message may be an individual message or may be added as an extension to *Registration Reply* and *Binding Acknowledgment* messages. Some embodiments of the FA and the MN may not use this message.

The structure of this message is shown in Fig. 6. The flags are discussed below.

Type. This is for various type indications.

A. This flag indicates if the buffer specifications provided by the MN (in the *Buffer Control Request* message) are rejected, accepted or partially accepted by the FA. The partial acceptance of the buffer specifications may occur if the FA's system resource can not accommodate all the requirements requested by the MN. If this option is selected, the available buffer resources of the FA should, in the present embodiment, be sent by the appropriate extensions (e.g. *Buffer Size* Extension or a *Buffer Lease Time* extension) to the MN.

A = 0, The FA accepts the buffer specifications.

A = 1, The FA partially accepts the buffer specifications. New specifications are sent with the appropriate extensions.

A = 2, The FA rejects the buffer specifications.

Sender IP Address. The IP address of the FA.

Identification. A 64-bit number, constructed by the MN and sent in a *Buffer Control Request* or *Registration Request* message. It is used for identifying the response to a *Buffer Control Request* or *Registration Request* message. It is also used as a protection from replay attacks.

3. *Buffer Size Extension*

This extension defines the size of the buffer that should be allocated for the mobile node by the agent or the size of the buffer that is offered by the agent to the mobile node.

The structure of this message is shown in Fig. 7. The flags are discussed below.

Type. This is for various type indications.

Length. The length of this extension in number of bytes.

Size. The size of the buffer required by the MN or the size of the buffer offered by the FA to the MN. The size is of 1K increments.

4. *Buffer Lease Time Extension*

This extension defines a lease time of the buffer that should be allocated to the mobile node by the mobile agent or the lease time of the buffer that is offered by mobile agent to the mobile node.

The structure of this message is shown in Fig. 8. The flags are discussed below.

Type. This is for various type indications.

Length. The length of this extension in number of bytes.

Lease Time. The lease time of the buffer required by the mobile node or the lease

5   time of the buffer offered by the mobile agent to the mobile node. The lease time is counted

in seconds and the value 0XFFFFFFFF is a reserved number to indicate infinite time.

5. *IP Filter Extension*

This extension is used to filter (e.g., discard) the data packets destined for the MN

10   based on their source IP addresses and the packet Identification field.

The structure of this message is shown in Fig. 9. The flags are discussed below.

Type. This is for various type indications.

Length. The length of this extension in number of bytes.

IP Count. The number of IP addresses listed in this extension.

15   C. This flag indicates if the FA should buffer the packets that have the same or

different source IP addresses listed in this extension. This flag should be checked only for

those IP addresses that do not include any IP IDs in this extension.

        C = 0, buffer or forward packets that have the same IP addresses as listed in

        this extension.

20   C = 1, buffer or forward packets that do not have the same IP addresses as

        listed in this extension.

IP Address(s). The IP address(s) included in this extension.

ID Count. The number of IP identifications included per IP address.

IP Index. This field uniquely identifies an IP address from the list of the IP

25   addresses included in this extension. The value of this field corresponds to the sequence

number (starting at zero) in which a particular IP address is listed. For example, if this field

contains zero (0), then it identifies the first IP address listed in this extension. Hence, all IP

IDs corresponding to that IP address are included in a tuple:

        <IP Index = 0, ID Count = n, IP ID1 ... IP IDn>,

30   where n is the number of IP IDs for this particular IP address. Similarly, if an IP Index field

contains two (2), then all the IP IDs listed following the tuple:

        <IP Index = 2, ID Count = n, IP ID1 ... IP IDn>

correspond to the third IP address listed in this extension.

If a particular IP address does not have any IP IDs, then the sequence number of that IP address should not, in the present embodiment, be present in the list of IP Index fields. For example, if the second IP Address listed does not have any IP IDs, then any IP Index with a value of one (1) should not, in the present embodiment, be present in this extension. If any IP address listed in the this extension is not identified by the IP Index field, then all of those IP addresses should, in the present embodiment, be completely filtered (based on the C flag).

IP ID. The IP identification(s) included for the IP address identified by an IP Index. If the very last IP ID happens to be in the lower 16 bytes, then the upper 16 bytes should, in the present embodiment, be padded.

6. *Authentication Extension*

This extension is used to authenticate *Buffer Control Request* and *Buffer Control Response* messages, only if they are sent independently (that is, they are not sent as extensions to a *Registration Request* or *Binding Update* message) .

This extension has the same format and default algorithm support requirements as the *Authentication* Extensions (MN-FA, MN-HA, HA-FA) defined in the base Mobile IP. However, it should, in the present embodiment, have its own type.

An authenticator value may also be included. The authenticator value can be computed from the stream of bytes including the shared secret key, payload, prior extensions, and the type and length of this extension.

Mobile Node Considerations

The MN may send the *Buffer Control Request* message to the FA as a separate message or as an extension to a *Registration Request* message. The MN may receive the *Buffer Control Response* from the FA as a separate message or as an extension to the Registration Reply message.

The MN should, in the present embodiment, explicitly notify the FA (e.g., via the *IP Filter* extension) if the buffering needs to be discriminated based on the source IP address and/or the IP Identification field.

The MN may add two *Buffer Control Request* extensions to a single *Registration Request* message while sending it to a FA. This situation may occur when a MN needs to notify a new FA to allocate a buffer, and at the same time, the MN needs to notify the previous FA (e.g., via the new FA) to forward buffered data. The MN should, in the present embodiment, also include a *Previous FA Notification* extension to this *Registration Request* message. In this case, the MN should set the B bit (B = 1) in the *Buffer Control Request* message that is destined for the new FA. The MN should also set the F bit(F = 1) in the *Buffer Control Request* message that is destined for the previous FA.

Foreign Agent Considerations

The FA may receive the *Buffer Control Request* from a MN as a separate message or as an extension to a *Registration Request* message. The FA may send a *Buffer Control Request* message to another FA as a separate message or as an extension to a *Binding Update* message.

The FA may send the *Buffer Control Response* to a MN as a separate message or as an extension to the Registration Reply message.

The FA may receive two *Buffer Control* extensions in a single *Registration Request* message from a MN. This *Registration Request* should, in the present embodiment, also include a *Previous FA Notification* extension. The FA should, in the present embodiment, allocate the buffer resources for the MN according to the specifications provided by the *Buffer Control Request* that has its B bit set (B = 1). The FA should, in the present embodiment, send the other *Buffer Control Request* that has its F bit set (F = 1) to the previous FA (as detailed in the *Previous FA Notification* extension) as an extension to the *Binding Update* message.

The FA, by default, should, in the present embodiment, buffer all the packets destined for the MN unless otherwise specified by the *IP Filter* extension.

The FA should, in the present embodiment, follow the format of these messages as described herein.

Buffer Management
1. Storing Data

The data stored in the buffer is managed according to the type of buffer mentioned in the T field of the *System Change Request* message. If the length of the buffer is fixed as mentioned in the L field of the *Buffer Control Request* message then the data will be stored in the buffer using a FIFO (First In First Out) policy. If and when the buffer gets full, data at the front of the buffer (the oldest data) is discarded to make room for new data inserted at the end of the buffer.

If the length of the buffer is variable and the buffer is full then the system will try to expand the size of the buffer to accommodate the new coming data. If the expansion is impossible then the data at the front of the buffer is discarded to make room for new data. The discarded data will be lost unless the F flag was set (F = 1) in the *Buffer Control Request* Message. In that case, the data will be forwarded to the new FA.

2. Buffer Allocation

One of the following cases occurs during buffer allocation when the MN sends *Buffer Control Request* message to the FA with A bit set to 1 (one):

1   - If no buffer is allocated for the MN then the allocation of buffer will be handled as follows:

- If the K is set to 0 (zero) and the MN includes the *Buffer Size* extension and/or *Buffer Lease Time* extension, then the buffer is allocated according to the size and the lease time mentioned in these extensions.

- If, however, the FA is unable to accommodate the specifications (size, lease time etc.) requested by the MN, the default values are then used to allocate the buffer.

- If either one or all of these extensions are not included then the FA's default values are used to allocate the buffer.

- If the K flag is set to 1 (one) and the MN's requested buffer specifications (included in the *Buffer Size* extension and/or *Buffer Lease Time* extension) can not be accommodated by the FA, then it (the FA) should, in the present embodiment, suggest its own buffer specifications (size, lease time etc.) to the MN through the *Buffer Control Response* message using the appropriate extensions. At the same time, the FA should, in the present embodiment, allocate those suggested buffer resources for the MN.

- If the new buffer specifications (size, lease time, etc.) sent by the FA are not acceptable to the MN, then the MN may send a new *Buffer Control Request* message to the FA with the new specifications.

- If the FA receives a *Buffer Control Request* message with both A and B flags set to 1 (one), the allocation of the buffer is done first followed by the start of buffering of all the appropriate packets that are destined for the MN.

- If the FA receives a *Buffer Control Request* message for a MN that has already allocated buffer, the FA then re-allocates the buffer according the most recent *Buffer Control Request* message.

3. Forwarding Data

Upon receiving a *Buffer Control Request* message with $F = 1$ and $D = 1$, the FA should, in the present embodiment, delete the buffer allocated to the MN after forwarding the entire buffer. Future packets received after this message are lost.
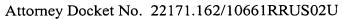
Upon receiving a *Buffer Control Request* message with $F = 1$ and $D = 0$, the FA should, in the present embodiment, delete the buffer allocated to the MN after forwarding the entire buffer. Future packets received after this message are immediately (without being buffered) forward to the MN. The filtering rules (if any) specified while allocating the buffer should, in the present embodiment, be kept in place. The forwarding will continues until the lease time expires.

4. Buffer Deletion

The buffer will be implicitly deleted if the lease time expires. It will be explicitly deleted if the MN sends a *Buffer Control Request* message with the D flag set to 1 (one).

Conclusion

The present invention provides a unique system and method that manages packets and other types of data in handoff situations, such as those that occur in a Mobile IP network. It is understood that the above disclosure provides many different embodiments, or examples, for implementing different features. Techniques and requirements that are only specific to certain embodiments should not be imported into other embodiments. Also, specific examples of networks, components, and formats are described below to simplify the

present disclosure. These are, of course, merely examples and are not intended to limit the invention from that described in the claims.